19. Функция Эйлера: значение на степени простого числа, явный вид

Функция Эйлера

Лемма 4

Функция Эйлера мультипликативна, то есть, если $a, b \in \mathbb{N}$ взаимно просты, то $\varphi(ab) = \varphi(a)\varphi(b)$.

Доказательство. • Запишем числа от 1 до ab в таблицу $a \times b$ так, что в первой строке — числа от 1 до a, во второй — от $a + 1$ до $2a$, итд, в b строке — числа от $(b-1)a + 1$ до ba.

1	2	3	…	a-3	a-2	a-1	a
a+1	a+2	a+3	…	2a-3	2a-2	2a-1	2a
			…				
(b-1)a+1	(b-1)a+2	(b-1)a+3	…	ba-3	ba-2	ba-1	ba

b строк

• Все числа в i столбце принадлежат одному вычету $\bar{i} = i + a\mathbb{Z}$ по модулю a. Эти числа взаимно просты с a, если и только если $(i, a) = 1$.

• Вычеркнем все столбцы с номерами i, не взаимно простыми с a. Останутся ровно $\varphi(a)$ столбцов.

Пусть a = 8; b = 3.

PS функция Эйлера от 8 это 4 (нам подходят 1, 3, 5, 7)

функция Эйлера от 3 это 2 (нам подходят 1, 2)

функция Эйлера от 24 это 8 (нам подходят 1, 5, 7, 11, 13, 15, 17, 19)

1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
ПСВ 3		ПСВ 3		ПСВ 3		ПСВ 3	

То есть в этой табличке мы получили все варианты остатков по модулю ab.

• Все числа, взаимно простые с ab, должны быть взаимно простыми и с a, они лежат в оставшихся $\varphi(a)$ столбцах.

• Рассмотрим оставшийся столбец, пусть числа в нем имеют вид $j,\ a + j,\ \dots,\ (b-1)a + j$. Эти числа образуют ПСВ $(\mathrm{mod}\ b)$ в силу теоремы 13 (так как получены из ПСВ $0, 1, \dots, b-1$ умножением на a, взаимно простое с b и прибавлением j: $\quad 0 \to j,\ 1 \to a + j,\ \dots,\ b - 1 \to (b-1)a + j$).

• Значит, среди чисел j, $a+j$, ..., $(b-1)a+j$ ровно $\varphi(b)$ взаимно простых с b. Остальные числа точно не взаимно просты с ab, вычеркнем их.

• Оставшиеся $\varphi(a)\varphi(b)$ чисел взаимно просты и с a, и с b, а значит, взаимно просты с ab. Значит, осталось ровно $\varphi(ab)$ чисел (все числа от 1 до ab, взаимно простые с ab). $\square$

1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
ПСВ 3		ПСВ 3		ПСВ 3		ПСВ 3	

Лемма 5

Если $p \in \mathbb{P}$, $n \in \mathbb{N}$, то $\varphi(p^n) = p^n - p^{n-1}$.

Доказательство. • Посчитаем количество чисел от 1 до p^n, не взаимно простых с p^n.

• Пусть $(a, p^n) = d > 1$. Так как $p^n \vdots d$, должно быть $d \vdots p$.

• Следовательно, числа от 1 до p^n, не взаимно простые с p^n — это в точности числа от 1 до p^n, кратные p. Их количество равно $\frac{p^n}{p} = p^{n-1}$. $\square$

Комментарии: действительно, что у нас может быть не взаимно простого с простым числом в какой-то степени? Собственно, все числа, кратные p (то есть каждое p-тое). Их как раз p^{n-1}.

Теорема 16

Если $n \in \mathbb{N}$ имеет каноническое разложение $n = p_1^{k_1} \dots p_m^{k_m}$, то

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right) \dots \left(1 - \frac{1}{p_m}\right).$$

Доказательство. • Докажем индукцией по количеству простых делителей s, что $\varphi(p_1^{k_1} \dots p_s^{k_s}) = \prod_{i=1}^{s} \varphi(p_i^{k_i})$.

• База для $s = 1$ очевидна.

• Переход $s \to s+1$. Так как $(p_1^{k_1} \dots p_s^{k_s}, p_{s+1}^{k_{s+1}}) = 1$, по Лемме 4 и индукционному предположению имеем

$$\varphi(p_1^{k_1} \dots p_s^{k_s} \cdot p_{s+1}^{k_{s+1}}) = \varphi(p_1^{k_1} \dots p_s^{k_s}) \cdot \varphi(p_{s+1}^{k_{s+1}}) =$$
$$\left(\prod_{i=1}^{s} \varphi(p_i^{k_i})\right) \cdot \varphi(p_{s+1}^{k_{s+1}}) = \prod_{i=1}^{s+1} \varphi(p_i^{k_i}).$$

• Следовательно,

$$\varphi(n) = \prod_{i=1}^{m} \varphi(p_i^{k_i}) = \prod_{i=1}^{m} (p_i^{k_i} - p_i^{k_i-1}) = \prod_{i=1}^{m} p_i^{k_i}\left(1 - \frac{1}{p_i}\right) = n \cdot \prod_{i=1}^{m}\left(1 - \frac{1}{p_i}\right).$$

20. Сумма функции Эйлера по делителям числа.

Сумма функции Эйлера по делителям числа

Теорема 17

Для любого $n \in \mathbb{N}$ $\quad \sum\limits_{d \in \mathbb{N},\, d \,|\, n} \varphi(d) = n.$

Давайте немного посмотрим на примерах: пусть n = 12. Тогда сумма будет равна $\varphi(1) + \varphi(2) + \varphi(3) + \varphi(4) + \varphi(6) + \varphi(12)$ = 1+1+2+2+2+4 = 12

n = 14. . Тогда сумма будет равна $\varphi(1) + \varphi(2) + \varphi(7) + \varphi(14)$ = = 1+1+6+6 = 14

Пусть n = 13. Тогда $\varphi(1) + \varphi(13)$ = 13

Доказательство. • Рассмотрим все $\mathbb{N}$ числа от 1 до n — их как раз n штук. Каждое из них имеет НОД с n — и этот НОД — делитель n.

• Для любого $d \mid n$ подсчитаем количество всех чисел из $\{1, \ldots, n\}$, чей НОД с n равен d.

Число 14. Хотим для каждого делителя d посмотреть, сколько ({1, …, n}, n)=d. То есть для 14:

14 = 1*2*7, делители 14 – это 1, 2, 7, 14.

({1, …, 14}, 14) = 1, это выполняется для 1, 3, 5, 9, 11, 13, то есть таких 6 штук.

({1, …, 14}, 14) = 2, это выполняется для 2, 4, 6, 8, 10, 12, то есть таких 6 штук.

({1, …, 14}, 14) = 7, это выполняется для 7, то есть таких 1 штука.

({1, …, 14}, 14) = 14, это выполняется для 14, то есть таких 1 штука.

• Такие числа делятся на d, значит, их нужно искать среди $d, 2d, \ldots, n = \frac{n}{d}d$. Так как
$d = (kd, n) = (kd, \frac{n}{d}d) = d \cdot (k, \frac{n}{d}) \iff (k, \frac{n}{d}) = 1$,
количество чисел из $\{1, \ldots, n\}$, чей НОД с n равен d — это в точности количество таких $k \in \{1, \ldots, \frac{n}{d}\}$, что $(k, \frac{n}{d}) = 1$, а это количество равно $\varphi(\frac{n}{d})$.

k∈{1, 2, 7, 14}

$\varphi(1) + \varphi(2) + \varphi(7) + \varphi(14)$ = 14

• Если d пробегает все натуральные делители n, то $d' = \frac{n}{d}$ также пробегает все натуральные делители n. Поэтому,
$$n = \sum_{d \in \mathbb{N},\, d \,|\, n} \varphi(\tfrac{n}{d}) = \sum_{d' \in \mathbb{N},\, d' \,|\, n} \varphi(d'). \qquad \square$$

Другой вариант доказательства:

1 Случай: если n – простое число, то делители n – это 1 и, собственно, n. Тогда $\varphi(1) + \varphi(n) = n$.

2 Случай: если n – составное число, n = $p_1^{\alpha_1} * p_2^{\alpha_2} * p_3^{\alpha_3} * p_4^{\alpha_4} * \ldots * p_s^{\alpha_s}$ (каноническое разложение)

Заметим одну интересную вещь:

$\varphi(1) + \varphi(p) + \varphi(p^2) + \varphi(p^3) + \cdots + \varphi(p^l)$= $1 + (p - p^0) + (p^2 - p) + (p^3 - p^2) + \cdots + (p^l - p^{l-1}))$

Телескоп ☺, останется только p^l.

$$n = \left(\varphi(1) + \varphi(p_1) + \varphi(p_1^2) + \cdots + \varphi\left(p_1^{\alpha_1}\right)\right) * \left(\varphi(1) + \varphi(p_2) + \varphi(2) + \cdots + \varphi\left(p_2^{\alpha_2}\right)\right) * \ldots * (\varphi(1) + \varphi(p_s) + \varphi(p_s^2) + \cdots + \varphi(p_s^s))$$

Если раскрыть скобки, будут получаться слагаемые вида $\varphi(p_i) * \varphi(p_j) * \ldots * \varphi(p_q)$, но вследствие мультипликативности функции Эйлера получим $\varphi(p_i * p_j * p_q)$, где произведение p-шек это делитель n.

21. Кольцо вычетов и его обратимые элементы. Поле вычетов по простому модулю.

Кольцо вычетов

• Вычеты по модулю $m \in \mathbb{Z}$ — они же вычеты по модулю идеала $m\mathbb{Z}$ — образуют *кольцо вычетов* $\mathbb{Z}_m := \mathbb{Z}/m\mathbb{Z}$.

Лемма 6

Обратимые элементы $\mathbb{Z}_m$ — это в точности вычеты из ПрСВ $(\mathrm{mod}\ m)$.

ПрСВ – приведённая система вычетов, например: m = 42. Тогда приведенная система вычетов: 1, 5, 11, 13, 17, 19, 23, 25, 29, 31, 37, 41. (то есть числа из полной системы вычетов, но взаимно простые с m)

Доказательство. • Если $\bar{a} \in \mathbb{Z}_m$ обратим, то существует такой $\bar{b} \in \mathbb{Z}_m$, что $\bar{a}\bar{b} = \bar{1} \iff ab \equiv_m 1$. Тогда $(ab, m) = 1$, а значит и $(a, m) = 1$.

• Наоборот, пусть $(a, m) = 1$. По Теореме 13 тогда $0, a, 2a, \ldots, (m-1)a$ — ПСВ $(\mathrm{mod}\ m)$. Значит, $\exists b :\ ab \equiv_m 1 \Rightarrow \bar{a}\bar{b} = \bar{1}$. □

Комментарии: как мы знаем, (наверное, привет сравнению по модулю идеала). Если ab и m отличаются на 1, то, конечно, они взаимно простые. Если выкинем b, никаких новых делителей точно не появится, поэтому НОД останется 1. Вот мы и получили, что $\bar{a}$ это вычет из ПрСВ (mod m)

(обратим, если имеет обратный)

• Если вычет $\overline{a}$ обратим, то обратный вычет $(\overline{a})^{-1}$ единственен (это доказано в общем случае для кольца ранее, а в данном случае следует из доказательства Леммы 6).

Теорема 18

Если $p \in \mathbb{P}$, то $\mathbb{Z}_p$ — поле.

Доказательство. Так как все некратные p числа взаимно просты с p, ПрСВ $\pmod p$ — это все ненулевые вычеты. Тогда по Лемме 6, все ненулевые элементы $\mathbb{Z}_p$ обратимы.

Про кольцо нам уже сказали выше. Что нам не хватает для поля? Обратного элемента по умножению. А мы знаем, что ненулевые элементы обратимы.

22. Алгоритм поиска обратного вычета. Решение сравнения с одним неизвестным.

Алгоритм поиска обратного вычета

- Пусть $a \in \mathbb{Z}$, $m \in \mathbb{N}$, причем $(a, m) = 1$. Как найти обратный вычет a^{-1} ?
- Пусть r — остаток от деления a на m. Тогда $0 \leq r < m$.

$a = km + r$

Пусть у нас есть кольцо по модулю 26. Тогда ПрСВ: 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25.

Обратный вычет к 1 – это 1, 3 – это 9, 5 – это 21 и тд

m = 26

- Если $r = 0$, то $(a, m) > 1$ и обратного вычета не существует.
- Если $r > 0$, то с помощью алгоритма Евклида ищем $d = (r, m) = (a, m)$.

55 = 2*26 + 3, d = (3, 26) = 1

54 = 2*26 + 2, d = (54, 26) = 2, то есть к 54 нет обр вычета

1 = 55*x + 26y, x=9, y=-19 (как частный случай решения)

$55 * 9 \equiv 1(mod\ 26)$ (x это и есть вычет)

- Если $d > 1$, то обратного вычета не существует.
- Если $d = 1$, то при помощи (выполненного ранее) алгоритма Евклида ищем линейное представление НОД: $1 = ax + my$.
- Тогда $ax \equiv 1 \pmod{m}$, а значит, $(\overline{a})^{-1} = \overline{x}$ в $\mathbb{Z}_m$.

Линейное сравнение с одним неизвестным

- Пусть $a, b \in \mathbb{Z}$, $m \in \mathbb{N}$. Нужно решить (относительно x) сравнение
$$ax \equiv b \pmod{m}. \qquad (*)$$
- Пусть $d = (a, m)$. Если $b \not\vdots\, d$, то очевидно, $(*)$ решений не имеет.
- Если $b \,\vdots\, d$, то пусть $a = a'd$, $b = b'd$, $m = m'd$. Тогда
$$(*) \iff ax - b \,\vdots\, m \iff a'x - b' \,\vdots\, m' \iff a'x \equiv b' \pmod{m'}. \qquad (**)$$
- Так как $(a', m') = 1$, существует обратный вычет $(\overline{a'})^{-1}$ в $\mathbb{Z}_{m'}$.
- Пусть $s \in (\overline{a'})^{-1}$. Тогда $x \equiv b's \pmod{m'}$ — решение сравнения $(**)$, а значит, и исходного сравнения $(*)$.

$5x \equiv 15(mod\ 10)$

$d = (5, 10) = 5$

$6x \equiv 7(mod\ 2)$

$d =$ (6, 2) = 2, 7 на 2 не делится, ежу понятно, что решений нет

Дальше сокращаем на d:

$x \equiv 3(mod\ 2)$

(1, 2) = 1, существует обратный вычет для 1 в Z по m', то есть по 2. Это 1 в нашем случае. Тогда $x \equiv 3 * 1(mod\ 2)$– наше решение.

25. Алгоритмы поиска решения для КТО.

Алгоритмы поиска решения для КТО

• Пусть $m_1, \dots, m_k$ — попарно взаимно простые натуральные числа, $m = m_1 \dots m_k$, $a_1, \dots, a_k \in \mathbb{Z}$.

• Мы ищем такое a, что $a \equiv_{m_1} a_1$, ..., $a \equiv_{m_k} a_k$ $(*)$.

• Будет использоваться алгоритм поиска обратного вычета, описанный выше.

Алгоритм 1.

• Пусть $m'_i = \frac{m_1 \dots m_k}{m_i}$. Тогда $(m'_i, m_i) = 1$.
$b_i \in \{0, 1, \dots, m_i - 1\}$ — такое число, что $b_i \cdot m'_i \equiv 1 \pmod{m_i}$ (мы найдем b_i с помощью алгоритма поиска обратного вычета).

Утверждение

$a = a_1 b_1 m'_1 + a_2 b_2 m'_2 + \dots + a_k b_k m'_k$ — *решение* $(*)$.

Доказательство. Так как $m'_j \,\vdots\, m_i$ при всех $j \neq i$, для любого $i \in \{1, \dots, k\}$
$a \equiv a_i b_i m'_i \equiv a_i \pmod{m_i}$. □

• Как сказано выше, все решения системы $(*)$ — это в точности числа, сравнимые с a по модулю m.

• Поделив a на m с остатком, мы найдем решение системы среди чисел $0, 1, \dots, m - 1$.

Алгоритм 2

• Индукцией по s найдем x_s, удовлетворяющее первым s сравнениям:

$x_s \equiv_{m_1} a_1, \ldots, x_s \equiv_{m_s} a_s$.

• База $s = 1$ очевидна: подойдет $x_1 = a_1$.

Переход $s \to s+1$. • Пусть $n_s = m_1 \ldots m_s$.

Будем искать решение в виде $x_{s+1} = x_s + c_s n_s$.

• Тогда $x_{s+1} - x_s \,\vdots\, m_j$ для всех $j \in \{1, \ldots, s\}$, поэтому, x_{s+1} удовлетворяет первым s сравнениям.

• Подберем c_s так, чтобы $x_{s+1} \equiv a_{s+1} \pmod{m_{s+1}}$:

$x_s + c_s n_s \equiv a_{s+1} \pmod{m_{s+1}} \iff c_s n_s \equiv a_{s+1} - x_s \pmod{m_{s+1}} \iff c_s \equiv (a_{s+1} - x_s) \cdot (n_s)^{-1} \pmod{m_{s+1}}$.

• Так как $(n_s, m_{s+1}) = 1$, обратный вычет $(n_s)^{-1}$ существует и может быть найден с помощью описанного выше алгоритма.

• Второй алгоритм решения КТО на первый взгляд сложнее, чем первый, но требует применения $k-1$ алгоритмов поиска обратного вычета (а не k): мы не ищем обратный вычет по модулю m_1.

• Поэтому, целесообразно нумеровать модули так, чтобы m_1 оказался самым большим.

26. Функция Мёбиуса. Сумма функции Мёбиуса по промежуточным делителям.

Функция Мёбиуса

Определение

Функция Мёбиуса $\mu(n) :=$

$$\begin{cases} 1, & \text{если } n = 1, \\ (-1)^k, & \text{если } n = p_1 \dots p_k \text{ — произведение различных простых чисел,} \\ 0, & \text{если } n \text{ делится на квадрат простого числа.} \end{cases}$$

Лемма 8

Пусть $m, d \in \mathbb{N}$, $m \vdots d$. *Тогда* $\sum\limits_{d\,|\,n\,|\,m} \mu(\frac{m}{n}) = \begin{cases} 1, & m = d, \\ 0, & m > d. \end{cases}$

(суммирование ведется по всем n*, кратным* d *и делящим* m*).*

Доказательство. • Пусть $k := \frac{m}{d} = p_1^{t_1} \dots p_r^{t_r}$ — каноническое разложение. Тогда

$$\sum_{d\,|\,n\,|\,m} \mu(\tfrac{m}{n}) = \sum_{s\,|\,p_1 \dots p_r} \mu(s) = \sum_{\ell=0}^{r} \mathrm{C}_r^{\ell}(-1)^{\ell} = (1-1)^r$$

(так как ненулевое значение μ достигается только на произведениях различных простых).

• Наша сумма равна 0 во всех случаях, кроме $r = 0$ (а это в точности $k = 1 \iff m = d$). В последнем случае сумма равна 1. □

Формула обращения Мёбиуса. Аддитивный вариант

Теорема 20

Пусть $f, g : \mathbb{N} \to$*, причем* $f(m) = \sum\limits_{d\,|\,m} g(d)$*. Тогда* $g(m) = \sum\limits_{n\,|\,m} \mu(\frac{m}{n}) f(n)$*.*

Доказательство.

$$\sum_{n\,|\,m} \mu\left(\frac{m}{n}\right) f(n) = \sum_{n\,|\,m} \mu\left(\frac{m}{n}\right) \cdot \sum_{d\,|\,n} g(d) =$$

$$\sum_{d\,|\,m} \left(g(d) \cdot \sum_{d\,|\,n\,|\,m} \mu\left(\frac{m}{n}\right) \right) = g(m)$$

по Лемме 8. □

Функция Эйлера через формулу обращения Мёбиуса

Теорема 21

Пусть $n = p_1^{k_1} \dots p_s^{k_s}$ *— каноническое разложение числа* n. *Тогда* $\varphi(n) = n(1 - \frac{1}{p_1}) \dots (1 - \frac{1}{p_s})$.

Доказательство. • По Теореме 17, $\sum\limits_{d \in \mathbb{N},\ d \mid m} \varphi(d) = m$.

• По Формуле обращения Мёбиуса,
$\varphi(n) = \sum\limits_{d \in \mathbb{N},\ d \mid n} \mu(d) \cdot \frac{n}{d}$.

• Напомним, что при $d = p_{i_1} \dots p_{i_t}$ мы имеем $\mu(d) = (-1)^t$ (здесь $i_1, \dots, i_t$ — различные индексы), $\mu(1) = 1$, а в остальных случаях $\mu(d) = 0$. Поэтому,

$$\varphi(n) = n - \sum_{1 \le i \le s} \frac{n}{p_i} + \sum_{1 \le i_1 < i_2 \le s} \frac{n}{p_{i_1} p_{i_2}} - \sum_{1 \le i_1 < i_2 < i_3 \le s} \frac{n}{p_{i_1} p_{i_2} p_{i_3}} + \dots =$$

$$n\left(1 - \sum_{1 \le i \le s} \frac{1}{p_i} + \sum_{1 \le i_1 < i_2 \le s} \frac{1}{p_{i_1} p_{i_2}} - \sum_{1 \le i_1 < i_2 < i_3 \le s} \frac{1}{p_{i_1} p_{i_2} p_{i_3}} + \dots\right) =$$

$$n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_s}\right). \quad \square$$

Формула обращения Мёбиуса. Мультипликативный вариант

Теорема 22

Пусть K — поле, $f, g : \mathbb{N} \to K \setminus \{0\}$, причем $f(m) = \prod\limits_{d \,|\, m} g(d)$.

Тогда $g(m) = \prod\limits_{n \,|\, m} f(n)^{\mu(\frac{m}{n})}$.

Доказательство.

$$\prod_{n \,|\, m} f(n)^{\mu(\frac{m}{n})} = \prod_{n \,|\, m} \left(\prod_{d \,|\, n} g(d) \right)^{\mu(\frac{m}{n})} =$$

$$\prod_{d \,|\, m} g(d)^{\sum\limits_{d \,|\, n \,|\, m} \mu(\frac{m}{n})} = g(m)$$

по Лемме 8. $\square$

Сумма мультипликативной функции по делителям числа

Теорема 23

Пусть $f : \mathbb{N} \to$ *— мультипликативная функция,* $g(n) = \sum\limits_{d\,|\,n} f(d)$. *Тогда* g *— мультипликативная функция.*

Доказательство. • Пусть $a, b \in \mathbb{N}$, $(a, b) = 1$.

• $a = p_1^{k_1} \dots p_s^{k_s}$ и $b = q_1^{\ell_1} \dots q_t^{\ell_t}$ — канонические разложения.

• Так как $(a, b) = 1$, все эти простые различны и $ab = p_1^{k_1} \dots p_s^{k_s} q_1^{\ell_1} \dots q_t^{\ell_t}$ — каноническое разложение.

• По Теореме 8, $d \,|\, ab \iff d = p_1^{k'_1} \dots p_s^{k'_s} q_1^{\ell'_1} \dots q_t^{\ell'_t}$, где $0 \le k'_i \le k_i$ для всех $i \in \{1, \dots, s\}$ и $0 \le \ell'_j \le \ell_j$ для всех $j \in \{1, \dots, t\}$.

• Следовательно, $d = d_a d_b$, где $d_a \,|\, a$ и $d_b \,|\, b$, причем $(d_a, d_b) = 1$ и такое представление единственно: $d_a = p_1^{k'_1} \dots p_s^{k'_s}$ и $d_b = q_1^{\ell'_1} \dots q_t^{\ell'_t}$.

• Таким образом,

$$g(ab) = \sum_{d\,|\,ab} f(d) = \sum_{d_a\,|\,a} \sum_{d_b\,|\,b} f(d_a d_b) = \sum_{d_a\,|\,a} \sum_{d_b\,|\,b} f(d_a) f(d_b) =$$

$$\Big(\sum_{d_a\,|\,a} f(d_a)\Big)\Big(\sum_{d_b\,|\,b} f(d_b)\Big) = g(a)g(b). \qquad \square$$